TO: Interested Parties
FROM: Greg Lemon, Deputy Secretary of State
RE: Digital Signatures and E-Commerce Legislation
DATE: 11/18/03

I. Introduction

This memorandum deals in summary fashion with what are commonly referred to as digital signatures or electronic signatures. I prefer the term digital authentication to digital signature or electronic signature, because the goal really is it to make sure that transactions performed electronically are endorsed by the person who is who they purport to be, and that the document is not changed in transmission, or authenticating the document. A signature or its equivalent is not always really necessary for this purpose.

II. Traditional Signatures

Black's Law Dictionary defines signature as: "The act of writing one's name upon a deed, note contract, or other instrument, either to identify or authenticate it, or to give it validity as one's own act." Also "a sign stamp, or mark, impressed as by a seal, or the name of any person written in his own hand signifying that the writing preceding it accords with his own wishes and intentions"

At law a signature is used to prove that someone signed or endorsed a document. They create a presumption that the document was so signed or endorsed. That presumption can be rebutted through testimony or extrinsic evidence such as handwriting analysis or comparison.

III. Digital Authentication Laws

Nebraska Digital Signatures Act (Neb. Rev. Stat. §86-1701, effective July 13th, 2000)

1. Summary

In 1998 the legislature passed LB924, which included (among other things) the Nebraska Digital Signatures Act

The Nebraska Act is based on the California Digital Signatures Act (passed in 1996) with one important distinction--The California law only applies to transactions with government entities, the Nebraska law applies to both public and private transactions

What the law does

The Nebraska law gives a digital signature the full force and effect of a manual signature as long as certain requirements are met

The Nebraska law also allows the use of a digital signature in any instance where a manual signature is customarily used or required

The law is permissive--digital signatures are used with the consent of all parties to the transaction

What are the requirements for a digital signature to be valid under the act?

it must be:

Unique to the person using it;

Capable of verification;

Under the sole control of the person using it;

Linked to data in such a manner that if the data are changed, the digital signature is invalidated;

and

it must conform to rules and regulations adopted by the Secretary of State

The regulations recognize public key encryption and signature dynamics as valid under this act. They also specifically state the regulations and law does not supercede or invalidate digital signatures or validation done under any other law.

2. Electronic Signature Amendments (government filings)

In 2000 amendments to the Digital Signature Act generally were adopted to allow state and local government agencies to use pin numbers or other electronic identifiers for electronic filings, license renewals, etc. The pin number or electronic signature would not have to rise to the level of technical sophistication and security of a digital signature so long as the procedure is established by rule and regulations and certain requirements are met.

1) For any state agency that accepts filings, applications or other correspondence which by law or regulation requires a signature the agency may allow, pursuant to regulation promulgated by the Secretary of State, that such filings, etc. may be signed or endorsed by pin number, password, or other electronic identifier and submitted electronically provided the following prerequisites are met:

a. A risk assessment of the security of the method of filing and electronically filing versus related to the level of security needed to ensure the integrity of the filing is done.
c. An audit trail for the transaction is maintained (for example the address to which a pin number was sent, when it was sent, when it was used)

2) Nothing in the act would require the use of electronic filing and signatures unless otherwise specifically provided by law.

2. Scope

The digital signature portion of the law provides to any transaction in Nebraska.

The electronic signature/electronic filing portion of the law only applies to transactions with Nebraska Government entities.

These laws apply even if other specific law provides for a signature.

3. Interoperability/Comparison

Provides specific, but not exclusive, requirements for digital and electronic signature transactions. As long as these requirements are met you have a high degree of certainty that the transaction is legally binding and enforceable.

Does not stop anyone from using electronic signatures valid under other law (E-sign, UETA)

Uniform Electronic Transactions Act (Neb. Rev. Stat. §86-2101 through 86-2116, effective July 13th 2000)

1. Summary

The Uniform Electronic Transactions Act (UETA), which was drafted by the Commission on Uniform State laws and has been adopted in a number of states, is aimed at providing some legal

framework and certainty to electronic transactions. The law authorizes the use of electronic records and electronic signatures in any transaction.

UETA expressly validates electronic records, signatures and other contracts. It provides for the use of electronic records and information for retention purposes, providing certainty in this area. The act makes clear that the actions of machines ("electronic agents") programmed and used by people will bind the user of the machine, regardless of whether human review of the transaction occurred. It specifies the standards for sending and receiving electronic records, and it allows for innovation in financial services through the implementation of transferable records.

Electronic signature is defined as a sound, symbol, symbol or process logically associated with a record and executed or adopted by a person with the intent to sign the record. This could be as simple as an automated telephone instruction "if you would like to purchase this item press "9" now".

The act expressly states that it does not apply where other specific laws are in place, but only when no specific law governs the electronic transaction, so it does not interfere with existing or proposed state law on the subject, it fills in where the law is unclear.

2. Scope

This is Nebraska Law which applies to transactions in Nebraska of any kind, be they private, commercial or public. Although Nebraska specific, a number of other states have passed this law also so similar provisions apply in other states.

3. Interoperability/Comparison

This is a general law on electronic transactions, whereas the Nebraska Digital Signatures Act is specific. UETA does not apply where other specific requirements apply, for example, the law says the agreement must be in writing.

Electronic Signatures In Global and National Commerce Act (Effective October 1, 2000)

1. Summary

The Electronic Signatures In Global and National Commerce Act, also known as the "E-sign act" or "S.761A" Went into effect on October 1, 2000. The definition of electronic signature in this act is similar to that found in UETA, and the act provides that transactions shall not be denied legal force and effect strictly because they are in electronic format or electronically validated.

2. Scope

The E-sign act specifically applies to transactions in interstate and foreign commerce. It has similar provisions to UETA which state that a transaction shall not be denied legal force and effect solely because it is in electronic form.

Doesn't apply to UCC transactions or transactions relating to wills and testamentary trusts or adoption, divorce or family law.

3. Interoperability/Comparison

Many lawyers are spending many hours figuring out the interoperability of the E-Sign Act, UETA, and specific state provisions on digital or electronic signature requirements.

Very generally speaking E-sign pre-empts local laws on digital and electronic signatures and electronic transactions. However, the law also has a reverse pre-emption clause concerning UETA. The law states that in jurisdictions that have passed UETA as it was approved by the Commission on Uniform State laws, the UETA provisions apply rather than the e-sign provisions. However, UETA and E-sign provisions are very similar where they overlap. E-sign pre-empts any state law that specifically gives greater legal force and effect to digital or electronic signatures created by a specific technology. It should be noted that the Nebraska Digital Signatures act does not invalidate electronic or digital signatures valid under any other law.

E-sign has more consumer protection provisions than UETA, such as having people consent to having disclosures provided in electronic format.

IV. Digital Authentication Technologies

Basic Electronic Signatures:

Most simple example a pin number or password

Public Key Encryption

"asymmetric cryptosystem"—private key encrypts, public key decrypts, or decodes the document--Relies on encryption and security

Vendors(examples): Verisign, Digital Signatures Trust

Signature Dynamics:

Records the signature and sometimes other information (such as the speed at which it is written)

Biometrics:

Fingerprint Scan

Retina Scan

Hand Scan

Hybrids:

Rely on a combination of encryption and biometrics or signature dynamics.
Vendors(examples): SecuGen, PenOp, AproveIt

V. Other Issues

An additional issue that may needs to be dealt with in the digital authentication world is authority or capacity and integrity of endorsed documents. Many documents depend on more than just the name of the person in order to be validly authenticated. For example, I could sign a deed over to make you owner of the Empire State Building, or sign a contract giving you royalties based on the gross sales of all Microsoft Products. My signature would be valid, and my intent might even be sincere, but in addition to a question that could be raised about my sanity, the documents would be without force and effect because I don't serve in a capacity or have the authority to do the things the documents purport to do. Digital authentication could address some of these issues through the use of digital certificates for entities such as corporations or real time verification of authority through access to databases on the internet or intranets, for example.

Protecting the integrity of endorsed documents that exist purely in electronic form is an additional challenge in the digital world. Obviously it is very easy to alter the text of most digital documents, and generally not as easy to detect as altering a paper document. Encryption can be used to make it more difficult to change a document that is produced, transmitted or stored electronically.

BOTTOM LINE

The greatest degree of certainty and enforceability for electronic transaction in Nebraska is achieved using a digital certificate from a Nebraska approved certification authority. You may think of the Nebraska law and regulations as a form or template to be used in creating valid electronic transactions.

E-sign and UETA say that a transaction may not be denied legal effect solely because it is in electronic format or electronically signed. Exactly what constitutes a valid electronic signature or electronic transaction under the new law will be settled over many years by custom and usage, as well as the inevitable litigation. However, the items that will be looked at in determining the enforceability of these transactions will be intent or knowledge of the parties, uniqueness of the signature, and how the signature is tied to or associated with the transaction.

Just as with manual signatures, where we have different levels of authentication requirements based upon the document endorsed, there are and should be different levels of authentication requirements in the world of digital authentication.

How your particular business or enterprise should use electronic or digital signatures should be determined by weighing the benefits gained (speed, convenience) versus any security risks or financial liability associated with the transaction you will be using the technology with.

TIPPING POINT

This section is a later to addendum to this memo that was primarily written in the year 2000. Digital authentication laws in Nebraska and elsewhere have been for the most part written in a technology neutral fashion, based on the realization that technology moves much faster then legislatures and the goal of the legislation is to enable and encourage e-commerce and e-government, not hold it back.

The area of digital authentication has not really evolved or reached a tipping point where one particular method suddenly reaches a critical mass and suddenly becomes the default used and accepted generally in one or more particular area.

One of the reasons for this is that the private sector, generally a larger (and faster) driver of such things may not have as large a need for digital authentication as the public sector. While the public sector cares and needs proof of who they issue a driver's, doctor's or engineer's license to, Amazon.com, for example, is really primarily concerned with receiving payment and where to deliver the product sold. For those purposes, a credit card number serves well and is broadly used.

In order to provide a global solution for government, particularly in those situations where it is a point of first contact (and a pin number or password cannot be issued, which is much easier for a renewal than an initial license where it would add a step), some states have adopted, and Nebraska is considering the use of some unique identifiers known or likely to be know only by the person being authenticated and some government agencies or trusted third parties. These identifiers could be, for example, a combination of driver's license number, last four digits or entire Social Security Number, and date of birth, could be used to verify identity of "cold" callers visiting over the internet and wanting to use E-government services.

Supplementary Information

Approved Certification Authorities in Nebraska:

Digital Signature Trust Co.

255 North Admiral Byrd Road
Salt Lake City, Utah 84116-3703
Phone: : 888 294-7831
Fax: 801 326-5448

www.digsigtrust.com

Approved License #CA002

ID Certify, Inc.

209 Sixth Avenue North
Seattle, WA 98109
Phone: 206 956-8008
Fax: 206 956-8596

www.idcertify.com

Approved License #CA003

Links to Nebraska Digital Signature Information can be found at the Nebraska Secretary of State's Website

http://www.nol.org/home/SOS/digitalsig/digsig.htm